UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/611,771	06/30/2003	Juan A. Garay	Garay-10-1 (LCNT/125336)	2190

46363 7590 07/26/2007
PATTERSON & SHERIDAN, LLP/
LUCENT TECHNOLOGIES, INC
595 SHREWSBURY AVENUE
SHREWSBURY, NJ 07702

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
07/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/611,771	**Applicant(s)** GARAY ET AL.
	Examiner Carlton V. Johnson	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 May 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) *2,5,8,11-22,26-29* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,4,6,7,9,10 and 23-25* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed **5-10-2007**.

2. Claims **1 - 29** are pending. Claims **1, 3, 4, 6, 7, 9, 10, 23, 24, 25** have been amended. Claims **2, 5, 8, 11 - 22, 26 - 29** have been cancelled. Claims **1, 23** are independent.

Response to Remarks

3 The following is in response to papers filed on 5/10/2007.

3.1 The previous 112 issues based on formula processing have been resolved. The formulas have been removed from the claim language.

3.2 The term, "iteration", does not appear within the specification or original claims. (see Remarks Page 7, 8) There is no disclosure of an iteration of values transferred between users. This term has been used repeated within the amendments to the claimed invention. Paragraphs [0032], [0039] disclose the structure of a sequence but do not disclose the iteration of transfers between the two users. This appears to be new matters. If applicant feels there is disclosure for this claim limitation, please indicate the required citations for confirmation. The term, "iteration", will be interpreted to be a sequence of values such as generated by the Micali prior art.

3.3 Applicant argues that the referenced prior art does not disclose, a sequence. (see remarks Pages 7 - 9)

The claimed invention merely discloses a sequence with the current value based on the preceding value. A sequence is defined as a series, which is a number of things or events arranged in order and connected by being alike in some way. (see Merriam Webster Dictionary, 2005, ISBN-13: 978-0-87779-636-7) The Micali prior art discloses the generation of random numbers, but the random numbers are still in a sequence. Therefore, it satisfies the limitation of the claim.

3.4 Applicant argues the obviousness of the ASOKAN and Micali prior art combination. (see Remarks Page 8)

Applicant is reminded that the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

3.5 The examiner has considered the applicant's remarks concerning a method and system for a fair exchange of user information over a network by the transmission of user information encoded in association with a hidden value selected as one of a plurality of values distributed in a sequence wherein a difference between adjacent ones of said values increases and decreases symmetrically about one of the values of a known order. Applicant's arguments have thus been fully analyzed and considered but they are not persuasive.

After an additional analysis of the applicant's invention, remarks, and a search of the available prior art, it was determined that the current set of prior art consisting of **ASOKAN** (**20020049601**) and **Micali** (**4,944,009**) discloses the applicant's invention including disclosures in Remarks dated May 10, 2007.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims **1, 3, 4, 6, 7, 9, 10, 23 - 25** are rejected under 35 U.S.C. 103(a) as being unpatentable over **ASOKAN et al.** (US PGPUB No. **20020049601**) in view of **Micali et al.** (US Patent No. **4,944,009**).

Regarding Claim 1, ASOKAN discloses a method for fairly exchanging a hidden value of a first user for a hidden value of a second user, by a series of exchanges between the first user and the second user leading up to completing said hidden values, comprising the steps of:

c) iteratively exchanging the sequence values of the first and second users, progressing in a predetermined order toward an end of said sequence values; (see ASOKAN paragraph [0142], line 1; paragraph [0143], line 1: exchange a sequence of values in a predetermined order)

d) completing the exchange provided that the total number of iterations are completed, and terminating the exchange if the total number of iterations are not completed. (see ASOKAN paragraph [0072], lines 1-5; paragraph [0073], lines 1-2: complete exchange or error termination)

ASOKAN discloses wherein establishing a modulus and a modular function known to the first user and known to the second user, said modular function iteratively producing a plurality of sequence values. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose wherein each said sequence value is related.

However, Micali discloses:

a) wherein each said sequence value is related, according to said modular function, to a next previous sequence value, whereby conformance to the modular function can be determined for adjacent ones of the plurality of sequence values; (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. progressively increasing and decreasing); col. 12, lines 45-48: Blum integers; col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. root and modulus), modular function)

b) establishing a total number of iterations over which the sequence values will be exchanged between the first user and the second user; (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. value of known order, total number of iterations))

In addition, Micali discloses wherein difference values between adjacent ones of said sequence values are symmetrically distributed about one of said values of a known order. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation; col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the generation of a symmetrically distributed sequence for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18: " ... *To maintain the security of the system, longer sequences are best used with each encryption, and different sequences are best used in successive encryptions.* ... ")

Regarding Claim 3, ASOKAN discloses the method of claim 1. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically discloses said plurality of values are determined according to the modular function a root value and a modulus value. However, Micali discloses wherein the plurality of values are determined in accordance with a root value and a modulus value. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. root and modulus), modular function; col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the generation of a sequence based on root and modulus values, and utilized in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claim 4, ASOKAN discloses the method of claims 1, 11. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose said sequence values are determined. However, Micali discloses wherein said sequence values are determined as: over a known order equal to the total number of iterations, wherein each said sequence value is a result of the modular function applied to a next previous sequence value, raised to a power related to a difference in position between said sequence value and a respective beginning and end of the order. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. progressively increasing and decreasing, value of known order, total number of iterations); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the usage of a sequence generation algorithm within a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claim 6, ASOKAN discloses the method of claim 4. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose the usage of Blum integers. However, Micali discloses wherein said modulus value is a product of Blum integers. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. progressively increasing and decreasing); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the generation of Blum integers for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claim 7, ASOKAN discloses the method of claims 6. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose said Blum integers are selected from a group. However, Micali discloses wherein said Blum integers comprise related prime numbers. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. progressively increasing and decreasing); col. 12, lines 45-48: Blum integers (prime numbers))

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the usage of Blum integers for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures.

(see Micali col. 4, lines 15-18)

Regarding Claims 9, ASOKAN discloses the method of claims 1, wherein said hidden value is a value immediately preceding a last value of said sequence. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose said hidden value is a value immediately preceding a last value of said sequence. However, Micali discloses wherein said hidden value is a value immediately preceding a last value of said sequence. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. hidden value immediately preceding last value); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the generation of a sequence value for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claim 10, ASOKAN discloses the method of claims 1. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not disclose said number of iterations is at least 80. However, Micali discloses wherein said order value of known order is at least 80. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. order value of known order, total number of iterations); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the generation of a sequence utilizing a value of known order for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claim 23, ASOKAN discloses a system for exchanging user information over a network comprising:

a) at least one programmed processor coupled to a memory and arranged for conducting a fair exchange of a hidden value of a first user for a hidden value of a second user, by a series of exchanges between the first user and the second user leading up to completing said hidden values; (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications; paragraph [0002], lines 1-6: electronic commerce (computer system, processor utilized for commerce information))

d) iteratively exchanging the sequence values of the first and second users, progressing toward an end of said sequence values; (see ASOKAN paragraph

[0142], line 1; paragraph [0143], line 1: exchange a sequence of values in a predetermined order)

e) completing the exchange provided that the total number of iterations are completed and terminating the exchange if the total number of iterations are not completed. (see ASOKAN paragraph [0072], lines 1-5; paragraph [0073], lines 1-2: complete exchange or error termination)

ASOKAN does not specifically disclose a total number of iterations for fair exchange. However, Micali discloses:

b) establishing a modulus and a modular function known to the first user and known to the second user, said modular function iteratively producing a plurality of sequence values wherein each said sequence value is related, according to said modular function, to a next previous sequence value, whereby conformance to the modular function can be determined for adjacent ones of the plurality of sequence values; (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. progressively increasing and decreasing); col. 12, lines 45-48: Blum integers; col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. root and modulus), modular function)

c) establishing a total number of iterations over which the sequence values will be exchanged between the first user and the second user, (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. value of known order, total number of iterations))

In addition, ASOKAN does not specifically disclose a plurality of values distributed in a sequence wherein a difference between adjacent ones of said values increases and decreases symmetrically about one of said values of a known order, and said values in said first set have increasing differences between adjacent ones of said values.

However, Micali discloses wherein a plurality of values distributed in a sequence wherein a difference between adjacent ones of said values increases and decreases symmetrically about one of said values of a known order, and said values in said first set have increasing differences between adjacent ones of said values. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. progressively increasing and decreasing); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to the utilization of a processor, and to enable the generation of a sequence for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures (see Micali col. 4, lines 15-18).

Regarding Claim 24, ASOKAN discloses the system of claim 23, further comprising a further processor and wherein said processor and said further exchange said sequence values on behalf of the first and second users, respectively. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications to transfer values)

Regarding Claim 25, ASOKAN discloses the system of claims 23, wherein said processor is operable to effect the series of exchanges on a timed-basis. (see ASOKAN paragraph [0081], lines 2-5: timer (i.e. timed-basis) utilized in information transfers)

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

7/22/07

C.J.
CVJ
July 9, 2007